DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **24 Jan 13**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Fortinet, Incorporated FortiWiFi-60C Release (Rel.) 4.3.6

References: (a) Department of Defense (DoD) Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability (IO) test certification.

2. The FortiWiFi-60C Rel. 4.3.6 is hereinafter referred to as the System Under Test (SUT), meets all critical IO requirements for joint use within the Defense Information System Network (DISN) as a wireless product. The SUT met all critical IO requirements set forth in Reference (c); using test procedures derived from Reference (d). The SUT is certified and approved for joint use within the DISN. The operational status of the SUT must be verified during deployment. Any new discrepancies that are discovered in the operational environment will be evaluated for impact and adjudicated to the satisfaction of the Defense Information System Agency (DISA) via vendor Plan of Action and Milestones (POA&M) to address the concern (s) within 120 days of identification. No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect IO, but no later than three years from the date of this memorandum.

3. This finding is based on IO testing conducted by JITC, Indian Head, Maryland, from 1 through 8 February 2012. The DISA Certifying Authority (CA) has provided a positive Recommendation on 18 December 2012 based on the security testing completed by DISA Information Assurance (IA) test teams and published in a separate report, Reference (e).

4. The interface, Capability Requirements (CR), Functional Requirements (FR), and component status of the SUT are listed in Tables 1 and 2. The threshold Capability/Functional (CR/FR) requirements for Wireless Products are established by Section 5.3.1 of Reference (c) and were used to evaluate the IO of the SUT. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
WLAS					
802.11a	N	5.3.1.7.2.3	1, 2, 3, 5, and 7	Not Certified	See note 3.
802.11b	N	5.3.1.7.2.3		Not Certified	See note 3.
802.11g	N	5.3.1.7.2.3		Not Certified	See note 3.
802.16	N	5.3.1.7.2.3		NA	See note 4.
802.3i	N	5.3.1		Not Certified	See note 3.
802.3u	N	5.3.1		Not Certified	See note 3.
802.3z	N	5.3.1		NA	See note 4.
802.3ab	N	5.3.1		NA	See note 4.
WAB					
802.11a	N	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11b	N	5.3.1.7.2.3		Certified	
802.11g	N	5.3.1.7.2.3		Certified	
802.16	N	5.3.1.7.2.3		NA	See note 4.
802.3i	N	5.3.1		Certified	
802.3u	N	5.3.1		Certified	
802.3z	N	5.3.1		NA	See note 4.
802.3ab	N	5.3.1		NA	See note 4.
WEI					
802.11a	N	5.3.1.7.2.3	1, 3, and 4	NA	Products tested did not include WEIs.
802.11b	N	5.3.1.7.2.3		NA	
802.11g	N	5.3.1.7.2.3		NA	
802.16	N	5.3.1.7.2.3		NA	

NOTES:
1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).
2. The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3, System Functional and Capability Requirements.
3. The SUT provides WLAS functionality. This functionality is not certified because of outstanding test discrepancies adjudicated to be critical to certification. These discrepancies are not applicable to providing the wireless bridge functionality.
4. The SUT does not provide these conditionally required interfaces.

LEGEND:

ASLAN	Assured Services LAN	SUT	System Under Test
CR	Capability Requirement	UCR	Unified capabilities Requirements
FR	Functional Requirement	WAB	Wireless Access Bridge
N	No	WEI	Wireless End Instrument
NA	Not Applicable	WLAS	Wireless LAN Access System

Table 2. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Met	See note 2.
	WiFi Certified	Required (See note 3.)		Met	See note 4.
	Redundancy	Required		Met	
	FIPS 140-2 Level 1	Required		Met	See note 4.
	Latency	Required		Met	
	Traffic Prioritization	Required		Met	
	Wireless STIGs	Required		Met	See note 5.
2	**WIDS**				
	Continuous Scanning	Required	5.3.1.7.2.2	Not Met	See note 6.
	Location-sensing	Required	5.3.1.7.2.2	Not Met	See note 6.
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 7.)	5.3.1.7.2.3	Met	
	802.11 Interface Standards	Required (See note 8.)		Met	
	802.16 Interface Standards	Required (See note 9.)		NA	See note 10.
	Fixed/Nomadic WEIs	Required (See note 11.)		NA	See note 12.
4	**WEIs**				
	VoIP Solution	Required (See note 13.)	5.3.1.7.2.4	NA	
	Access Methods	Required (See note 14.)			
	Call Control Authentication	Required (See note 13.)			
	Call Termination	Required (See note 11.)			
5	**WLAS**				
	Loss of Call upon WLAS failure	Required (See note 15.)	5.3.1.7.2.5	Met	See note 16.
	Maximum supported EIs			Not Met	See notes 16 and 17.
	MOS			Not Met	See notes 16 and 17.
	Roaming			Met	See note 16.
6	**WAB**				
	Individual Interface Standards	Required (See note 8.)	5.3.1.7.2.6	Met	For specified interfaces
	Maximum Voice Calls Transported				See notes 16 and 17.
	Voice MOS				See note 16.
	E2E BER				
	Secure Voice Transmission				See note 16.
	Call Signaling Transport				See note 16.
	Latency				
	Jitter				
	WLAS/WLAB Combination				
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	Met	

Table 2. SUT CRs and FRs Status (continued)

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Vendor demonstrated IPv6 QoS and IPv6 packet transfer via Ethernet.
3. Only applies to 802.11 interfaces.
4. Verified via vendor LoC.
5. Vendor met STIG requirements with submitted mitigations.
6. Not Supported at time of test.
7. Individual sub-requirements apply to specific interface types.
8. Applicable to 802.11 interfaces only.
9. Applicable to 802.16 interfaces only.
10. SUT does not provide an 802.16 interface.
11. Applies to WEIs; not applicable to WLASs or WABs.
12. SUT does not include WEIs.
13. The WEI is certified in conjunction with a call-control agent (VoIP solution).
14. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).
15. Specified requirements are only applicable to WLAS products.
16. Verified via emulated phone (Ixia).
17. The SUT supports the ability to limit the number of subscribers, thereby controlling number of voice subscribers.

LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz	MOS	Mean Opinion Score
802.16	IEEE series of wireless broadband standards	QoS	Quality of Service
ASLAN	Assured Service Local Area Network	STIG	Security Technical Implementation Guide
BER	Bit Error Rate	SUT	System Under Test
CR	Capability Requirement	UCR	Unified Capabilities Requirements
E2E	End-to-End	VoIP	Voice over Internet Protocol
EIs	End Instruments	WAB	Wireless Access Bridge
FIPS	Federal Information Processing Standard	WEI	Wireless End Instrument
FR	Functional Requirement	WIDS	Wireless Intrusion Detection System
GHz	Gigahertz	WiFi	trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including WLAN
IEEE	Institute of Electrical and Electronics Engineers		
ID	Identification	WLAS	Wireless LAN Access System
IPv6	Internet Protocol version 6		
LoC	Letter of Compliance		

5. In accordance with the Program Manager's request, JITC did not develop a detailed test report. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program, which .mil/.gov users can access on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool at http://jit.fhu.disa.mil (NIPRNet). Information related to Approved Products List (APL) testing is available on the DISA APL Testing and Certification website located at http://www.disa.mil/Services/Network-Services/UCCO. All associated test information is available on the DISA Unified Capability Certification Office APL Integrated Tracking System (APLITS) website located at https://aplits.disa.mil.

6. The JITC point of contact is Mr. Kevin Holmes; commercial (301) 743-4300; e-mail address is Timothy.K.Holmes.civ@mail.mil. The JITC's mailing address is 3341 Strauss Ave., Ste. 236, Indian Head, MD 20640-5035. The tracking number for Fortinet, Inc. FortiWiFi-60C Rel. 4.3.6 is 1122011.

FOR THE COMMANDER:

Adam K. Britt

3 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
Defense Information Systems Agency, TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 3," September 2011
(d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)"
(e) Joint Interoperability Test Command, "Information Assurance (IA) Fortinet FortiWiFi60C Rel. 4 DRAFT IA Assessment Report TN 1122011"

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Fortinet Incorporated (Inc.) FortiWiFi-60C Release (Rel.) 4.3.6 (Tracking Number 1122011) hereinafter referred to as the System Under Test (SUT).

2. SPONSOR. Mr. Michael Caruso, Marine Corps Network Operations and Security Center Enterprise Services, 27410 Hot Patch Road, Quantico, VA 22134, e-mail: michael.caruso@mcnosc.usmc.mil.

3. SYSTEM POC. Mr. Carl Erickson, 42616 St. Clair Lane, Leesburg, VA 20176, e-mail: cerickson@fortinet.com.

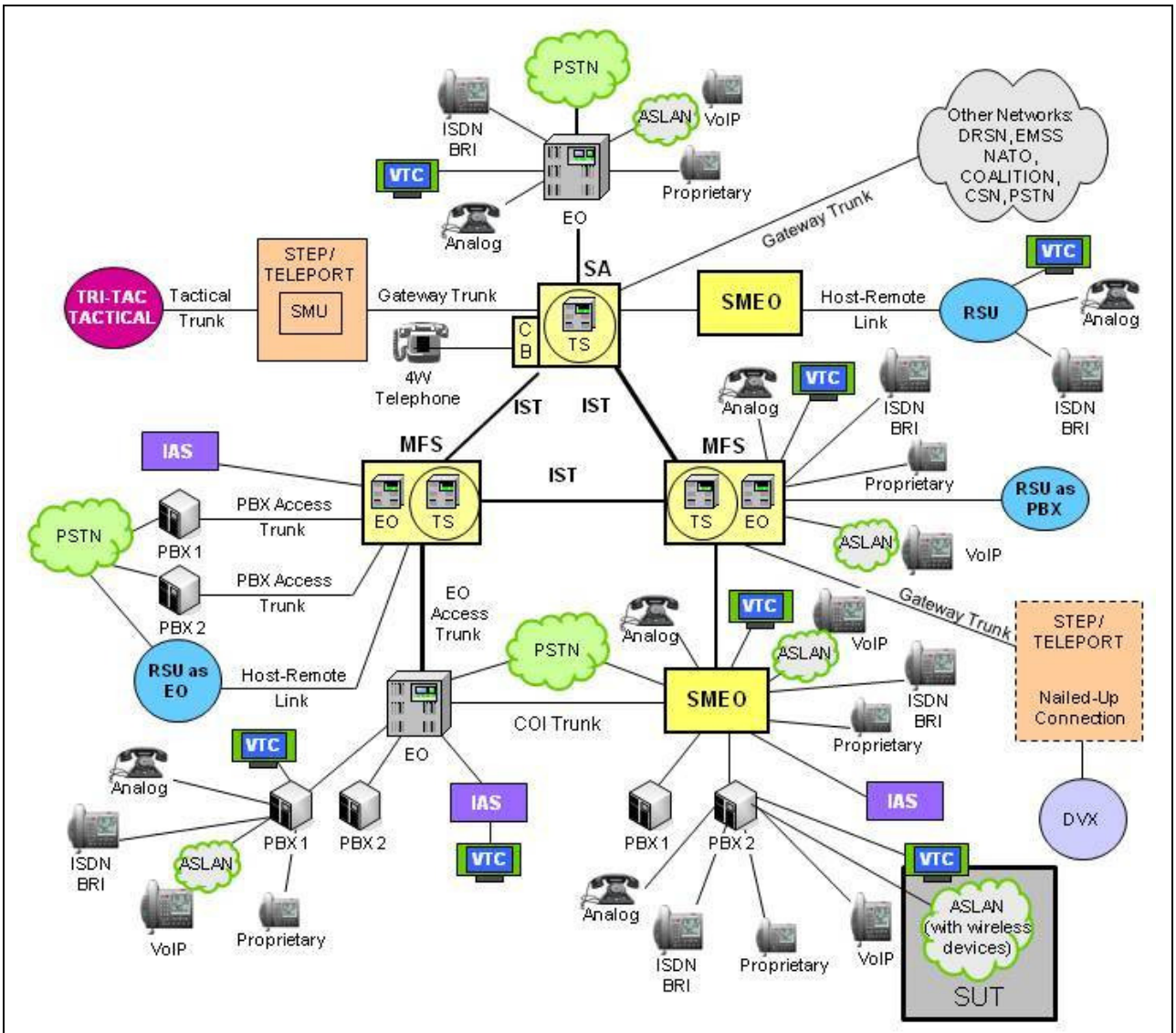
4. TESTER. Joint Interoperability Test Command (JITC), Indian Head, Maryland.

5. SYSTEM DESCRIPTION. Wireless device product implementations are considered extensions of the Local Area Network (LAN) physical layer. The Unified Capabilities (UC) Requirements (UCR) defines three wireless products: Wireless End Instruments (WEI), Wireless LAN Access Systems (WLAS), and Wireless Access Bridges (WAB).

The SUT supports Ethernet interfaces that provide 1 Gigabit per second firewall throughput, two Gigabit Ethernet (GbE) Wide Area Network ports, and five GbE Local Area Network (LAN) ports. In addition to the physical Ethernet ports, the SUT offers dual-band wireless networking capabilities and support for 802.11a/b/g/n standards to provide secure wireless network connections. The wireless device requirements applied to the SUT are reported in a separate certification document.

The SUT is a Wireless LAN (WLAN) access point for 802.11a/b/g/n wireless devices, and uses Federal Information Processing Standards (FIPS) 140-2 validated encryption for backhaul (point-to-point) and mesh (point-to-multipoint) applications.

6. OPERATIONAL ARCHITECTURE. The UCR Defense Switched Network (DSN) architecture in Figure 2-1 depicts the relationship of the SUT to the DSN switches.



LEGEND:

4W	4-Wire
ASLAN	Assured Services Local Area Network
BRI	Basic Rate Interface
CB	Channel Bank
COI	Community of Interest
CSN	Canadian Switch Network
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
MFS	Multi-Function Switch
NATO	North Atlantic Treaty Organization
PBX	Private Branch Exchange
PBX 1	Private Branch Exchange 1
PBX 2	Private Branch Exchange 2
PSTN	Public Switched Telephone Network
RSU	Remote Switching Unit
SA	Standalone
SMEO	Small End Office
SMU	Switched Multiplex Unit
STEP	Standardized Tactical Entry Point
SUT	System Under Test
Tri-Tac	Tri-Service Tactical Communications Program
TS	Tandem Switch
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing

Figure 2-1. DSN Architecture

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CR) and Functional Requirements (FR), Information Assurance (IA), and other requirements for wireless devices are established by Section 5.3.1 of Reference (c).

7.1 Interfaces. The wireless devices use interfaces to connect to the Assured Services Local Area Network (ASLAN) infrastructure and wireless devices (voice, video, and data). The threshold requirements for interfaces specific to the wireless products are listed in Table 2-1.

Table 2-1. Wireless Device Interface Requirements

Interface	Critical (See note1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Criteria	Remarks
WLAS					
802.11a	N	5.3.1.7.2.3	1, 2, 3, and 5	Meet minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	N	5.3.1.7.2.3	1, 2, 3, and 5		
802.11g	N	5.3.1.7.2.3	1, 2, 3, and 5		
802.16	N	5.3.1.7.2.3	1, 2, 3, and 5	Meet minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.
802.3i	N	5.3.1	1, 2, 3, and 5	Meet minimum CR/FRs and 802.3 interface standards.	Provides wired ASLAN access and NM interface.
802.3u	N	5.3.1	1, 2, 3, and 5		
802.3z	N	5.3.1	1, 2, 3, and 5		
802.3ab	N	5.3.1	1, 2, 3, and 5		
WAB					
802.11a	N	5.3.1.7.2.3	1, 2, 3, and 6	Meet minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	N	5.3.1.7.2.3	1, 2, 3, and 6		
802.11g	N	5.3.1.7.2.3	1, 2, 3, and 6		
802.16	N	5.3.1.7.2.3	1, 2, 3, and 6	Meet minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.
802.3i	N	5.3.1	1, 2, 3, and 6	Meet minimum CR/FRs and 802.3 interface standards.	Provides wired ASLAN access and NM interface.
802.3u	N	5.3.1	1, 2, 3, and 6		
802.3z	N	5.3.1	1, 2, 3, and 6		
802.ab	N	5.3.1	1, 2, 3, and 6		
WEI					
802.11a	N	5.3.1.7.2.3	1, 2, 3, and 6	Meet minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	N	5.3.1.7.2.3	1, 2, 3, and 6		
802.11g	N	5.3.1.7.2.3	1, 2, 3, and 6		
802.16	N	5.3.1.7.2.3	1, 2, 3, and 6	Meet minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.

NOTES:
1. "Required Definition" means "Conditionally Required." The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements.
2. The detailed CR/FR requirements are contained in Table 2-2. The CR/FR numbers represent a roll-up of UCR requirements. Enclosure 3 provides a list of more detailed requirements for security device products.

LEGEND:

ASLAN	Assured Service Local Area Network	NM	Network Management
CR	Capability Requirement	SUT	System Under Test
FR	Functionality Requirement	UCR	Unified Capabilities Requirements
ID	Identification	WAB	Wireless Access Bridge
LAN	Local Area Network	WEI	Wireless End Instrument
N	No	WLAS	Wireless LAN Access System
NA	Not Applicable	Y	Yes

7.2 CR and FR. Wireless device products have required and conditional features and capabilities that are established by Section 5.8 of the UCR. The SUT does not need to provide non-critical (conditional) requirements. If they are provided, they must function according to the specified requirements. The SUTs features and capabilities and its aggregated requirements in accordance with (IAW) the wireless device requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of Enclosure 3.

Table 2-2. Wireless CRs and FRs

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3
	WiFi Certified	Required (See note 2.)	5.3.1.7.2.1		
	Redundancy	Required	5.3.1.7.2.1		
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1		
	Latency	Required	5.3.1.7.2.1		
	Traffic Prioritization	Required	5.3.1.7.2.1		
	Wireless STIGs	Required	5.3.1.7.2.1		
2	**WIDS**				
	Continuous Scanning	Required	5.3.1.7.2.2	See Table 3-1 of Enclosure 3	Applies to WLAS and WAB products
	Location-sensing	Required	5.3.1.7.2.2		
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 3.)	5.3.1.7.2.3	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3
	802.11 Interface Standards	Required (See note 4.)			
	802.16 Interface Standards	Required (See note 5.)			
	Fixed/Nomadic WEIs	Required (See note 6.)			
4	**WEIs**				
	VoIP Solution	Required (See note 7.)	5.3.1.7.2.4	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3
	Access Methods	Required (See note 8.)			
	Call Control Authentication	Required (See note 6.)			
	Call Termination	Required (See note 6.)			
5	**WLAS**				
	Loss of Call upon WLAS failure	Required (See note 7.)	5.3.1.7.2.5	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3	Applies to WLAS only
	Maximum supported EIs	Required (See note 7.)			
	MOS	Required (See note 7.)			
	Roaming	Required (See note 7.)			

Table 2-2. Wireless CRs and FRs (continued)

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
6	**WAB**				
	Individual Interface Standards	Required (See note 8.)	5.3.1.7.2.6	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3	Applies to WAB only
	Maximum Voice Calls Transported				
	Voice MOS				
	E2E BER				
	Secure Voice Transmission				
	Call Signaling Transport				
	Latency				
	Jitter				
	WLAS/WLAB Combination				
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	See Table 3-1 of Enclosure 3	

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Only applies to 802.11 interfaces.
3. Individual sub-requirements apply to specific interface types.
4. Applicable to 802.11 interfaces only.
5. Applicable to 802.16 interfaces only.
6. Applies to WEIs; not applicable to WLASs or WABs.
7. The WEI is certified in conjunction with a call-control agent (VoIP solution).
8. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).

LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz
802.16	IEEE series of wireless broadband standards
BER	Bit Error Rate
CR	Capability Requirement
E2E	End-to-end
EIs	End Instruments
FIPS	Federal Information Processing Standard
FR	Functional Requirement
GHz	Gigahertz
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol version 6
LAN	Local Area Network
MOS	Mean Opinion Score
STIG	Security Technical Implementation Guide
SUT	System Under Test
UCR	Unified Capabilities Requirements
VoIP	Voice over Internet Protocol
WAB	Wireless Access Bridge
WEI	Wireless End Instrument
WIDS	Wireless Intrusion Detection System
WiFi	trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including WLAN
WLAN	Wireless LAN
WLAS	Wireless LAN Access System

7.3 IA. The IA requirements for wireless device products are listed in Table 2-3. The IA requirements were derived from the UCR 2008, Section 5.3.1, ASLAN Infrastructure, and UCR 2008, Section 5.4, Information Assurance Requirements.

Table 2-3. Wireless Product IA Requirements

Requirement	Critical (See note.)	UCR Reference
WiFi Alliance Certified (802.11 only)	Yes	5.3.1.7.2.1
FIPS 140-2 Level 1/2	Yes	5.3.1.7.2.1
Wireless STIG Requirements	Yes	5.3.1.7.2.1
WIDS Monitoring	Yes	5.3.1.7.2.1
General Requirements	Yes	5.4.6.2
Authentication	Yes	5.4.6.2.1
Integrity	Yes	5.4.6.2.2
Confidentiality	Yes	5.4.6.2.3
Non-repudiation	Yes	5.4.6.2.4
Availability	Yes	5.4.6.2.5

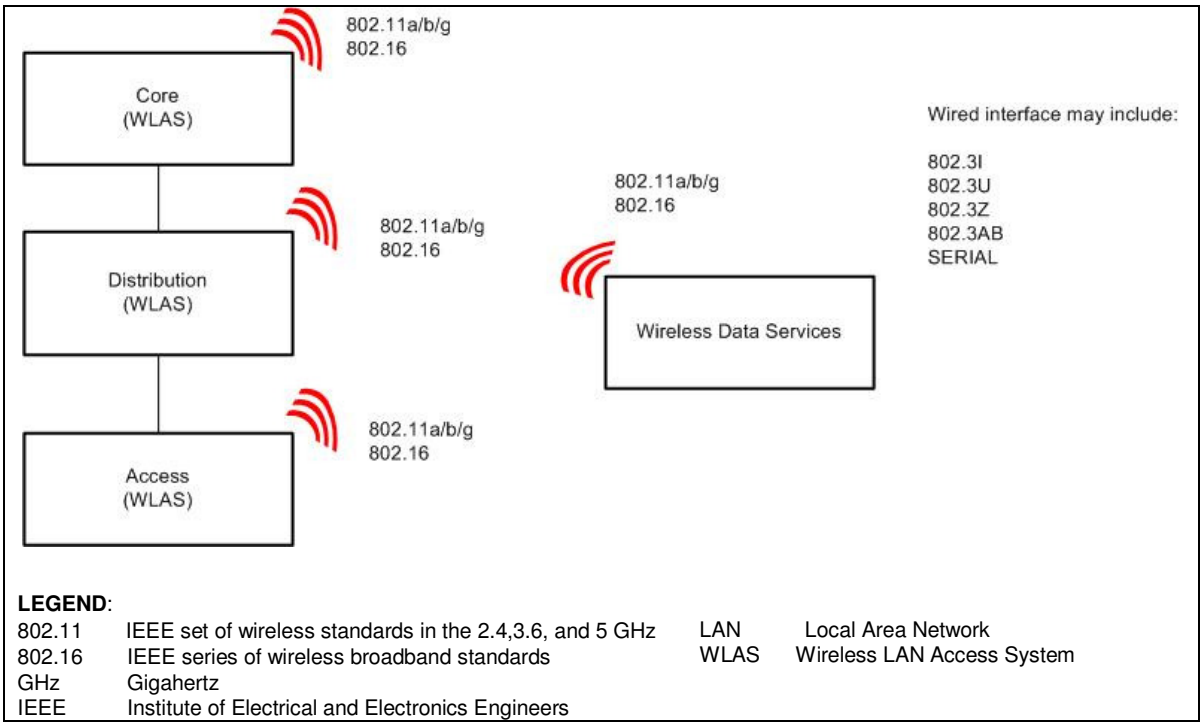
NOTE: Not all IA requirements from the referenced UCR section apply.

LEGEND:

FIPS	Federal Information Processing Standard	WIDS	Wireless Intrusion Detection System
IA	Information Assurance	WiFi	trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including WLAN
STIG	Secure Technical Implementation Guide		
UCR	Unified Capabilities Requirements		

7.4 Other. None.

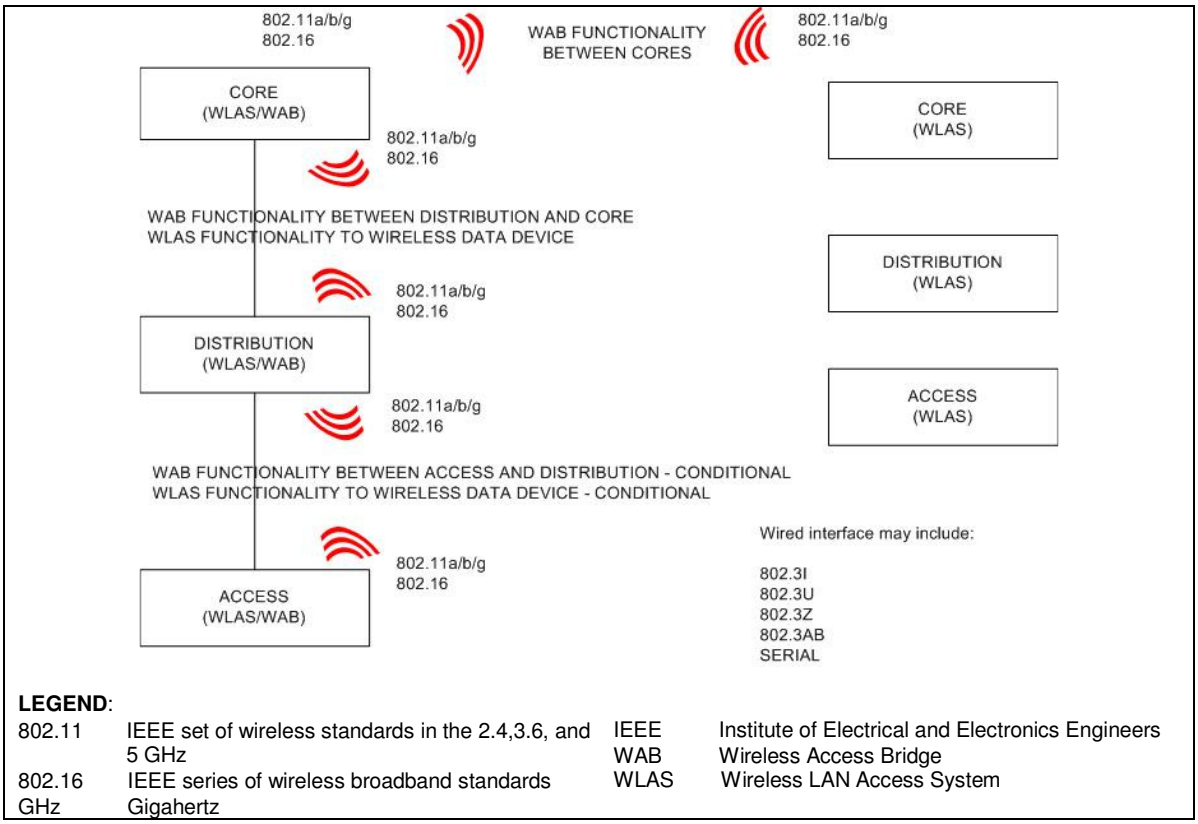
8. TEST NETWORK DESCRIPTION. The SUT was tested at its Indian Head, Maryland Test Facility in a manner and configuration similar to that of the DISN operational environment. Testing of the system's required functions and features was conducted using the test configurations depicted in Figures 2-2 through 2-4.



LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz	LAN	Local Area Network
802.16	IEEE series of wireless broadband standards	WLAS	Wireless LAN Access System
GHz	Gigahertz		
IEEE	Institute of Electrical and Electronics Engineers		

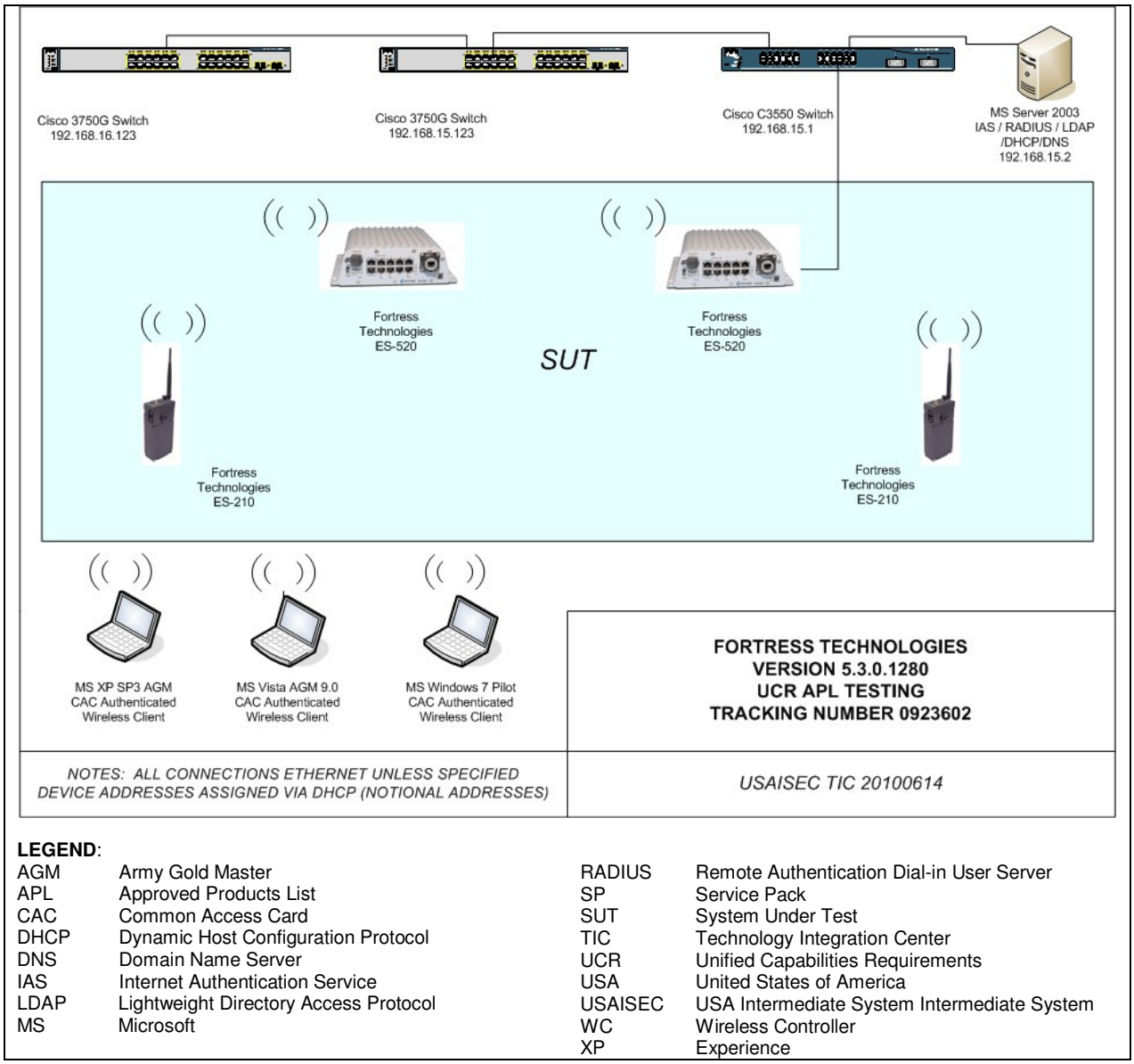
Figure 2-2. WLAS Test Configuration



LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz	IEEE	Institute of Electrical and Electronics Engineers
		WAB	Wireless Access Bridge
802.16	IEEE series of wireless broadband standards	WLAS	Wireless LAN Access System
GHz	Gigahertz		

Figure 2-3. WAB Test Configuration



LEGEND:

AGM	Army Gold Master	RADIUS	Remote Authentication Dial-in User Server
APL	Approved Products List	SP	Service Pack
CAC	Common Access Card	SUT	System Under Test
DHCP	Dynamic Host Configuration Protocol	TIC	Technology Integration Center
DNS	Domain Name Server	UCR	Unified Capabilities Requirements
IAS	Internet Authentication Service	USA	United States of America
LDAP	Lightweight Directory Access Protocol	USAISEC	USA Intermediate System Intermediate System
MS	Microsoft	WC	Wireless Controller
		XP	Experience

Figure 2-4. SUT Wireless Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine interoperability with a complement of ASLAN Infrastructure products. The ASLAN Infrastructure products listed are those used in the tested configuration. The list is not intended to identify only those ASLAN Infrastructure products that are certified for use with the SUT. The SUT is certified for use with any/all of the ASLAN Infrastructure products on the UC Approved Products List (APL).

Table 2-4. Tested System Configurations

System Name	Equipment		
Required Ancillary Equipment	Active Directory		
	Public Key Infrastructure		
	RADIUS		
	System Log Server		
Additional Equipment Needed	Management Workstation		
	LDAP Server		
Fortinet WiFi-60C Rel. 4.3.6	**Hardware**	**Card Name** **Part Number/Name**	**Software/Firmware**
	Management Workstation (site-provided)	NA	Windows XP SP3
			Firefox 12.0
			Tumbleweed 4.9.2.172
			ActiveClient CAC 6.1 x86
	Remote Workstation (site-provided)	NA	Windows XP SP3
			FortiClient 3.0.472
			Tumbleweed 4.9.2.172
			ActiveClient CAC 6.1 x86
	FortiWiFi-60C	NA	FortiOC v4.0 build 8920 MR3

LEGEND:

CAC	Common Access Card	RADIUS	Remote Authentication Dial-in User Server
NA	Not Applicable	SP	Service Pack
LDAP	Lightweight Directory Access Protocol	XP	Experience

10. TESTING LIMITATIONS.

a. Creation of a contention state in the wireless domain is not possible without violating the Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g standards. The absence of a contention state creates a technical challenge to confirm traffic policing functions. The 802.11 wireless protocols operate in a shared RF medium, half-duplex mode, regulating client transactions using time division access, thus mitigating wireless traffic contention. Currently, a traffic contention state is the only known trigger for the traffic policing function on network elements.

b. Testing of various traffic management parameters was conducted using up to 50 independent flow streams representing user network transaction densities significantly higher than practical (based on current wireless best business practices) wireless implementations. Current test equipment licensing constraints limit the overall number of flows that may be utilized.

c. End instruments (EI) and Department of Defense (DoD) secure communications devices were not available to support testing. Tests pertaining to those elements were not conducted. Representative measurements were recorded in place of actual test results. These measurements indicate a link quality that is both suitably high and represents a reasonably low risk affiliated with the use of these products.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for a WAB IAW Section 5.3.1.7.2 of the UCR and is certified for joint use with other ASLAN Infrastructure Products listed on the APL.

Additional discussion regarding specific testing results is contained in subsequent paragraphs.

11.1 Interfaces. The SUT's wireless interface statuses are provided in Table 2-5.

Table 2-5. Wireless Interface Requirements Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
WLAS					
802.11a	N	5.3.1.7.2.3	1, 2, 3, 5, and 7	Not Certified	See note 3.
802.11b	N	5.3.1.7.2.3		Not Certified	See note 3.
802.11g	N	5.3.1.7.2.3		Not Certified	See note 3.
802.16	N	5.3.1.7.2.3		NA	See note 4.
802.3i	N	5.3.1		Not Certified	See note 3.
802.3u	N	5.3.1		Not Certified	See note 3.
802.3z	N	5.3.1		NA	See note 4.
802.3ab	N	5.3.1		NA	See note 4.
WAB					
802.11a	N	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11b	N	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11g	N	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.16	N	5.3.1.7.2.3	1, 2, 3, 6, and 7	NA	See note 4.
802.3i	N	5.3.1	1, 2, 3, 6, and 7	Certified	
802.3u	N	5.3.1	1, 2, 3, 6, and 7	Certified	
802.3z	N	5.3.1	1, 2, 3, 6, and 7	NA	See note 4.
802.3ab	N	5.3.1	1, 2, 3, 6, and 7	NA	See note 4.
WEI					
802.11a	N	5.3.1.7.2.3	1, 3, and 4	NA	Products tested did not include WEIs.
802.11b	N	5.3.1.7.2.3	1, 3, and 4	NA	
802.11g	N	5.3.1.7.2.3	1, 3, and 4	NA	
802.16	N	5.3.1.7.2.3	1, 3, and 4	NA	

NOTES:
1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).
2. The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3, System Functional and Capability Requirements.
3. The SUT provides WLAS functionality. This functionality is not certified because of outstanding test discrepancies adjudicated to be critical to certification. These discrepancies are not applicable to providing the wireless bridge functionality.
4. The SUT does not provide these conditionally required interfaces.

LEGEND:

ASLAN	Assured Services LAN	SUT	System Under Test
CR	Capability Requirement	UCR	Unified capabilities Requirements
FR	Functional Requirement	WAB	Wireless Access Bridge
ID	Identification	WEI	Wireless End Instrument
LAN	Local Area Network	WLAS	Wireless LAN Access System
NA	Not Applicable		

11.2 CR and FR. The SUT's CR/FR status is listed in Table 2-6. The detailed CR/FR requirements are provided in Table 3-1 of the System Functional and Capability Requirements (Enclosure 3).

Table 2-6. SUT CR/FR Requirements Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Met	See note 2.
	WiFi Certified	Required (See note 3.)		Met	See note 4.
	Redundancy	Required		Met	
	FIPS 140-2 Level 1	Required		Met	See note 4.
	Latency	Required		Met	
	Traffic Prioritization	Required		Met	
	Wireless STIGs	Required		Met	See note 5.
2	**WIDS**				
	Continuous Scanning	Required	5.3.1.7.2.2	Not Met	See note 6.
	Location-sensing	Required	5.3.1.7.2.2	Not Met	See note 6.
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 7.)	5.3.1.7.2.3	Met	
	802.11 Interface Standards	Required (See note 8.)		Met	
	802.16 Interface Standards	Required (See note 9.)		NA	See note 10.
	Fixed/Nomadic WEIs	Required (See note 11.)		NA	See note 12.
4	**WEIs**				
	VoIP Solution	Required (See note 13.)	5.3.1.7.2.4	NA	
	Access Methods	Required (See note 14.)			
	Call Control Authentication	Required (See note 13.)			
	Call Termination	Required (See note 11.)			
5	**WLAS**				
	Loss of Call upon WLAS failure	Required (See note 15.)	5.3.1.7.2.5	Met	See note 16.
	Maximum supported EIs			Not Met	See notes 16 and 17.
	MOS			Not Met	See notes 16 and 17.
	Roaming			Met	See note 16.
6	**WAB**				
	Individual Interface Standards	Required (See note 8.)	5.3.1.7.2.6	Met	For specified interfaces
	Maximum Voice Calls Transported				See notes 16 and 17.
	Voice MOS				See note 16.
	E2E BER				
	Secure Voice Transmission				See note 16.
	Call Signaling Transport				See note 16.
	Latency				
	Jitter				
	WLAS/WLAB Combination				
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	Met	

Table 2-6. SUT CR/FR Requirements Status (continued)

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Vendor demonstrated IPv6 QoS and IPv6 packet transfer via Ethernet.
3. Only applies to 802.11 interfaces.
4. Verified via vendor LoC.
5. Vendor met STIG requirements with submitted mitigations.
6. Not Supported at time of test.
7. Individual sub-requirements apply to specific interface types.
8. Applicable to 802.11 interfaces only.
9. Applicable to 802.16 interfaces only.
10. SUT does not provide an 802.16 interface.
11. Applies to WEIs; not applicable to WLASs or WABs.
12. SUT does not include WEIs.
13. The WEI is certified in conjunction with a call-control agent (VoIP solution).
14. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).
15. Specified requirements are only applicable to WLAS products.
16. Verified via emulated phone (Ixia).
17. The SUT supports the ability to limit the number of subscribers, thereby controlling number of voice subscribers.

LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz	MOS	Mean Opinion Score
802.16	IEEE series of wireless broadband standards	STIG	Security Technical Implementation Guide
BER	Bit Error Rate	SUT	System Under Test
CR	Capability Requirement	UCR	Unified Capabilities Requirements
E2E	End-to-end	VoIP	Voice over Internet Protocol
EIs	End Instruments	WAB	Wireless Access Bridge
FIPS	Federal Information Processing Standard	WEI	Wireless End Instrument
FR	Functional Requirement	WIDS	Wireless Intrusion Detection System
GHz	Gigahertz	WiFi	trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including WLAN
IEEE	Institute of Electrical and Electronics Engineers		
IPv6	Internet Protocol version 6	WLAN	Wireless LAN
LAN	Local Area Network	WLAS	Wireless LAN Access System

a. General Wireless Requirements

(1) Internet Protocol Version 6 (IPv6). If an IP interface is provided in any of the wireless components, then it shall meet the IP requirements detailed in the DoD Profile for IPv6 IAW UCR 2008, Change 1, Section 5.3.1.7.2.1. The SUT WLAS (Figure 2-2) test configuration was used to investigate this requirement. The ES520 and ES210 support Secure Sockets Layer web management using both IPv4 and IPv6 addresses. Network testing confirms IPv6 packets are allowed to traverse the SUT in the WAB configurations without issue. Tests were conducted using the Ixia 250 test set and wired and wireless clients with Linux operating systems connected at various locations to confirm the Layer 2 transport of the IPv6 packets. Since the SUT operates at an Open System Interconnection Layer 2 level, all properly formatted Ethernet frames may traverse the system.

(2) WiFi (Trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including WLAN) Certified. All 802.11 wireless products must be WiFi Alliance Certified and shall be certified at the Enterprise level for WiFi Protected Access

Level 2 (WPA2) IAW UCR 2008, Change 1, Section 5.3.1.7.2.1. The JITC verified this requirement through vendor submitted Letter of Compliance (LoC).

(3) Redundancy. For wireless products that provide transport to more than 96 mission critical telephony users, the wireless products shall provide redundancy and WLAS and/or associated WLAN controller/ switches that provide and/or control voice services to more than 96 Wireless End Instruments (WEI) shall provide redundancy through either single product redundancy or dual product redundancy IAW UCR 2008 Change 1 Section 5.3.1.7.2.1. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. The SUT supports wireless controller failover between primary and subordinate controllers. Testers confirmed that each wireless controller listed was involved in a failed state and was the responsible recovery unit. Similarly, testers confirmed all the SUT Access Points (AP) listed support failover recovery. The AP and controller failovers were rapid and consistent. Testers confirmed assessment by observing a brief 1 ~ 2 Internet Control Message Protocol (ICMP) ping interruption on the wireless clients pinging to other network entities. (Note: The ping rate was one per second.)

(4) FIPS 140-2. All wireless connections shall be FIPS 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured IAW their wireless security profile. The JITC verified that the SUT met the requirements through vendor submitted LoC. The SUT is Level 1 certified.

(5) Latency. The use of wireless in the LAN shall not increase latency by more than 10 milliseconds (ms) above the specified maximum latency for a wired LAN IAW UCR 2008, Change 1, Section 5.3.1.7.2.1. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. Latency measurements for SUT WLAS, single unit acting as an access point: ES520 (servicing 802.11g clients): 36 milliseconds (ms) average, 1822 ms maximum. ES520 (servicing 802.11a clients): 12 ms average, 1028 ms maximum. ES210 (servicing 802.11a clients): 176 ms average, 2139 ms maximum. The Ixia Performance Endpoints (software agents installed on wireless clients reporting to the Ixia 250 test set) were used to record these measurements. Based on excessive latency, the WLAS functionality is not certified.

(6) Traffic Prioritization. The wireless products shall support LAN Traffic Prioritization and Quality of Service (QoS) IAW the following based on the wireless interface type IAW UCR 2008 Change 1 Section 5.3.1.7.2.1. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. A suitable test environment was not available to assess the traffic prioritization features of the SUT. Given operations in the wireless Radio Frequency domain, it is technically challenging to create an adequate contention state for the SUT to enforce traffic policing and shaping. The 802.11 wireless protocols operate in a shared medium, half-duplex mode, regulating client access, thus mitigating wireless traffic contention. Testers

confirmed the suitable transport of all appropriately-marked Differentiated Services Code Point (DSCP) traffic types traversing the SUT in each test configuration at various network ingress and egress points. All encoded DSCP tags traversed the SUT properly in each test configuration. Testers used both the Ixia 250 test set and wired and wireless Linux clients attached at various network ingress and egress points, confirming appropriate traffic capabilities.

(7) Wireless Security Technical Implementation Guide (STIG). Wireless products shall meet the WLAN security requirements as stipulated in the Wireless STIG and specified requirements of UCR 2008, Change 1, Section 5.3.1.7.2.1. The SUT meets the Wireless STIG requirements with mitigations, as detailed in the IA Findings report for this UC submission.

b. Wireless Intrusion Detection System (WIDS) Requirements. The WLAS and/or WAB wireless network shall be monitored by a WIDS. The WIDS system will have the following capabilities: 1) Continuous scanning. The WIDS will scan continuously around-the-clock to detect authorized and unauthorized activity. 2) Location-sensing WIDS. The WIDS will include a location sensing protection scheme for authorized and unauthorized wireless products. WIDS testing is not specified in the JITC UC Wireless Interoperability Test Plan. The WIDS is not supported in the ES520 and ES210 devices. Therefore, the following requirements are not applicable.

(1) Continuous Scanning. WIDS capabilities were not supported during testing in July 2010.

(2) Location-Sensing WIDS. WIDS capabilities were not supported during testing in July 2010. The ES210 supports an internal Global Positioning System (GPS) receiver along with an external GPS antenna connector. Integration of the geographic information is under development.

c. Wireless Interface Requirements.

(1) Interface Standards. If a wireless product is used, the wireless product shall support at least one of the following approved wireless LAN standards interfaces:

- 802.11a (WEI, WLAS, WAB)
- 802.11b (WEI, WLAS)
- 802.11g (WEI, WLAS, WAB)
- 802.16 (WEI, WLAS, WAB)

The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. The SUT has current WPA2 Certifications on file addressing the IEEE 802.11a/b/g modes. This is also collaborated in the SUT vendor's LoC. Testers confirmed successful wireless associations and SUT interoperability with four different vendor

wireless client interfaces. Tests were conducted successfully in each of the IEEE 802.11a/b/g modes. The SUT does not support IEEE 802.16 interfaces.

(2) Standards. Tests were conducted successfully in each of the IEEE 802.11a/b/g modes.

(3) 802.16 Interface Standards. The SUT does not provide the conditionally required 802.16 interfaces.

(4) Fixed/Nomadic WEIs. The SUT does not include the conditionally required WEIs.

d. WEI Requirements. The SUT does not include a WEI; therefore, WEI requirements are not applicable.

e. WLAS Requirements.

(1) Loss of Calls upon WLAS Failure. Failure of a WLAS shall not cause the loss of a call as the connection transfers from the primary to alternate system IAW UCR 2008, Change 1, Section 5.3.1.7.2.5. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. Testers successfully confirmed the SUT WLAS demonstrated the ability to maintain calls due to a failure of the WLAS (wireless controller and APs). Testers successfully confirmed Ixia performance endpoints by two methods: in conjunction with an Ixia 250 test set, and monitoring wireless client continuous ICMP pings to various network elements.

(2) Maximum Supported EIs. The WLAS shall support the maximum number of EIs per Table 5.3.1-8 of UCR 2008, Change 1, Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS. The SUT WLAS, ES520 and ES210, were not successful in supporting 50 voice calls IAW the listing for Access IP Trunk Pair with a link size of 10 Megabits per second (Mbps). (Refer to UCR 2008, Table 5.3.1-10, LAN Voice over IP Subscribers for IPv4 and IPv6). Testers determined the suitable product, link type, and link size to address the wireless IEEE 802.11a/b/g interfaces. Refer to the test limitations regarding EI availability and the 50-traffic-flow license constraint on the Ixia 250 test set. The SUT WLAS, ES520, achieved a Strategic level mean opinion score (MOS) = 4.02 with 50 voice calls using the test configuration where the ES520 supports access point functions with the 802.11g radio. This is the typical vendor-recommended configuration. The SUT WLAS, ES520, achieved a Strategic-to-Tactical level MOS = 3.6 with 50 voice calls using the test configuration where the ES520 supports access point functions with the IEEE 802.11a radio. This is an alternate configuration supported by the SUT. Both ES520 MOS measurements were associated with excessive latency, jitter, and packet loss, confirming the trend for distressed voice transport using the SUT. This represents a risk regarding the SUT's ability to support 96 simultaneous voice calls. The test measurements recorded with the ES210 did not satisfy the following requirements: MOS average = 2.8; latency average = 176 ms;

packet loss = 1.4 percent; and jitter = 9.4 ms. Thus, the ES210 is not suitable for UCR WLAS applications.

(3) MOS. IAW UCR 2008, Change 1, Section 5.3.1.7.2.5, the maximum number of telephones and/or other wireless non-voice EI products that the WLAS can support for the WLAS transmitter coverage distance is the point when voice quality degradation occurs. This degradation is defined as a MOS score below appropriate levels (i.e., Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2), when all telephones are off-hook simultaneously. The SUT WLAS, ES520, successfully supported a Strategic level MOS = 4.02 with 50 voice calls IAW the listing for Access IP Trunk Pair with a link size of 10 Mbps. The test configuration used the ES520 supporting access point functions with the 802.11g radio. This is the typical vendor-recommended configuration. The SUT WLAS, ES520, successfully supported a Strategic-to-Tactical level MOS = 3.6 with 50 voice calls IAW the listing for Access IP Truck Pair with a link size of 10 Mbps. This test configuration used the ES520 in an alternate configuration supporting access point functions with the IEEE 802.11a radio. The ES210, single IEEE 802.11a radio unit, did not meet the following WLAS requirement: MOS average = 2.8.

(4) Roaming. The WLAS shall not drop an active call as the WEI roams from one WLAS transmitter zone into another WLAS transmitter zone IAW UCR 2008, Change 1, Section 5.3.1.7.2.5. The SUT successfully sustained calls during transitions between APs. Transitions were measured at an average of 900 ms.

f. WAB Requirements.

(1) Individual Interface Standards. If provided, the WAB will be required to meet all the requirements for each individual type interface IAW UCR 2008, Change 1, Section 5.3.1.7.2.6. The SUT has current WPA2 Certifications on file addressing the IEEE 802.11a/b/g. This is also collaborated in the SUT vendor's LoC. Testers confirmed successful wireless associations and SUT interoperability with four different vendor wireless client interfaces. Tests were conducted successfully in each of the IEEE 802.11a/b/g modes for the ES520. The ES210 only supports IEEE 802.11a operations.

(2) Max Voice Calls Transported. The SUT WAB successfully supported 50 voice calls IAW the listing for Access IP Trunk Pair with a link size of 10 Mbps. (Refer to UCR 2008, Table 5.3.1-10, LAN VoIP Subscribers for IPv4 and IPv6.) Testers determined the suitable product, link type, and link size to address the wireless IEEE 802.11a/b/g interfaces. Refer to the test limitations regarding EI availability and the 50-traffic-flow license constraint on the Ixia 250 test set. MOS 4.4 represents suitable high quality transport. The latency, jitter, and packet loss measurements at higher traffic loading patterns confirm the trend for suitable transport using the SUT.

This represents a low risk regarding the SUT's ability to support 96 simultaneous voice calls.

(3) Voice MOS. The introduction of a WAB(s) shall not cause the End-to-End (E2E) average MOS to fall below appropriate levels (Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2) as measured over any 5-minute time interval IAW UCR 2008, Change 1, Section 5.3.1.7.2.6. The SUT WAB, ES520 and ES210 successfully supported a MOS = 4.4 with 50 voice calls IAW the listing for Access IP Trunk Pair with a link size of 10 Mbps. This was confirmed using the voice calls generated and received by the Ixia 250 test set.

(4) E2E Bit Error Rate (BER). The introduction of a WAB(s) shall not exceed the E2E digital BER requirement of less than one error in $1x10^{-8}$ (averaged over a 9-hour period) IAW UCR 2008, Change 1, Section 5.3.1.7.2.6. The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. Test equipment limitations constrained test results to characterize the quality of the data transport rather than a direct BER measurement. The quality of the data transport is representative of transport success regardless of payload encoded in the data frames. Testers interpreted the data loss measurements to be representative of suitably low BER measurements. Test duration = 9 hours, 0.0 percent byte loss.

(5) Secure Voice Transmission. The introduction of a WAB(s) shall not degrade secure transmission for secure end products, as defined in UCR 2008, Section 5.2.6, DoD Secure Communications Devices (DSCD). DSCDs were not available to support testing. The JITC did not have a call control agent or IP DSCD test capability. The JITC verified this requirement through emulated voice traffic using the Ixia test equipment suitably low latency, jitter, and packet loss measurements at higher traffic loading patterns confirm the trend for quality data transport using the SUT. This represents a low risk regarding the SUT's ability to support DSCD transmission.

(6) Call Signaling Transport. The WAB shall transport all call control signals transparently on an E2E basis IAW UCR 2008, Change 1, Section 5.3.1.7.2.6. The SUT is capable of supporting transport of signaling traffic. The JITC verified the requirement using Ixia test equipment because the test infrastructure did not include operational call control devices.

(7) Latency. The addition of a WAB(s) shall not cause the one-way delay measured from ingress-to-egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period IAW UCR 2008, Change 1, Section 5.3.1.7.2.6. The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. The SUT WAB, ES520 supports an average One Way Delay of 5 ms. The SUT WAB, ES210 supports an average One Way Delay of 4 ms. Testers confirmed these measurements using a variety of ingress and egress points for the Ixia 250 test set. Testing was performed on several wireless controllers and APs, thus ensuring consistent performance with each tested configuration.

(8) Jitter. The addition of the WAB shall not increase the LAN jitter requirements previously specified in UCR 2008, Change 1, Section 5.3.1. The JITC used SUT WAB test configuration to confirm this requirement. The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. The SUT WAB, ES520 supports an average jitter of 1.4 ms. The SUT WAB, ES210 supports an average jitter of 1.1 ms.

(9) WLAS/WAB Combination. The WLAS/WAB combination must meet all the requirements for access (WLAS) and bridging (WAB). The JITC used a modified SUT WAB test configuration to confirm this requirement. The SUT was configured for both bridging and access. The SUT WAB, acting simultaneously as a WLAS, met the requirement for supporting Service-Class Tagging/QoS as specified in UCR 2008, Change 1, Section 5.3.1.7.2.6. The SUT successfully transported the appropriate service-class-tagged traffic from a variety of network ingress and egress points. Testers confirmed the suitable transport of all appropriately marked DSCP traffic types traversing the SUT in each test configuration at various network ingress and egress points. All encoded DSCP tags traversed the SUT properly in each test configuration. Testers used both the Ixia 250 test set and (wired and wireless) Linux clients attached at various network ingress and egress points to confirm appropriate traffic classification capabilities. Testers confirmed the SUT could classify (encode) traffic with deliberate administrator-defined DSCP tags, using a traffic policy established on the management console. Testers used various network ingress and egress points to confirm that the DSCPs were appropriately modified by the SUT based on administrative policy.

g. ASLAN Requirements Applicable to Wireless Products.

(1) The wireless products must meet the general performance parameters applicable for access devices IAW UCR 2008, Change 1, Section 5.3.1.3. The SUT met the appropriate requirements as detailed in the previous paragraphs for the wireless interfaces. The JITC testers verified connectivity and UCR requirements for the wired interlaces. The SUT met the requirements for 10/100/1000 Mbps wired interfaces.

11.3 Information Assurance. The IA Assessment Report is published separately and is provided separately.

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. In accordance with the Program Manager's request, no detailed test report was developed. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents

and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil. (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The required and conditional features and capabilities for wireless products are established by Section 5.3.1.7.2 of the UCR. The SUT need not provide conditional features and capabilities; however, if they are present, they must function according to the specified requirements. The detailed Functional Requirements and Capability Requirements for wireless products are listed in Table 3-1.

Table 3-1. Wireless Products Capability/Functional Requirements

ID	Requirement	Reference	Remarks
	Wireless Requirements		
1	Meet the IP requirements detailed in the DISA UCR 2008 IPv6 Requirements.	5.3.1.7.2.1 (1)	All TP IO-1 (see IDs 363-491)
3	Wireless networks shall not be used to support special C2 users.	5.3.1.7.2.1 (3)	All TP IO-2
4	For wireless products that provide transport to more than 96 telephony users, the wireless products shall provide redundancy (single or dual).	5.3.1.7.2.1 (4)	All TP IO-3
6	The use of wireless in the LAN shall not increase latency by more than 10 ms above the specified maximum latency for a wired LAN.	5.3.1.7.2.1 (6)	All TP IO-4
7	Support LAN Traffic Prioritization: 802.11: 802.11e DSCP 802.16: 80216d and/or 802.16e	5.3.1.7.2.1 (7)	All TP IO-5
10	Wireless Interface Requirements: All 802.11: support 802.11e – Part 11and Amendments 6 and 8 802.11a: 802.11h Part 11 and Amendment 5 802.16 (fixed): 802.16d or 802.16e and Amendment 2 802.16 (nomadic): 802.16e and Amendment 2	5.3.1.7.2.3	All TP IO-6
11	WEIs shall: - Use 802.11 or 802.16 - Support dedicated or shared access method - Support authentication IAW IA - Provide telephone functionality identical to VoIP wired phone - Minimum FIPS 140-2 level 1 -VoIP timeout 0-60sec ; 5 sec default (VoIP device under test requirement)	5.3.1.7.2.4	WEI TP IO-7 For FIPs, see ID 236-Table E-9 Test Case 342
12	WLAS must support: - No loss of calls for primary failover to secondary WLAS - support max EIs as defined by MOS when all telephones are off hook simultaneously (table 5.3.1-9) -not drop active call when WEI roams from one WLAS to another.	5.3.1.7.2.5	WLAS/WEI Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non- redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS scores for strategic and tactical situations, in an open-air environment at a distance of 100 feet, except for the 5-second re-authentication as stated in item 1, (i.e., strategic MOS 4.0, strategic-to-tactical MOS 3.6, tactical-to- tactical MOS 3.2). TP IO-8
13	If WABs support 802.16 it must support 802.16d Part 16 or 802.16e part 16 and Amendment 2	5.3.1.7.2.6 (1)	WAB TP IO-9

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	Remarks
Wireless Requirements (continued)			
14	Max WAB voice calls IAW 5.3.1.7.3 Traffic engineering	5.3.1.7.2.6 (2)	WAB TP IO-10
15	The introduction of a WAB(s) shall not cause the end-to-end average MOS to fall below appropriate levels (strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2)	5.3.1.7.2.6 (3)	WAB As measured over any 5- minute time interval. TP IO-11
16	The introduction of a WAB(s) shall not exceed the end-to-end digital BER requirement of less than 1 error in $1x10^{-8}$ (averaged over a 9-hour period).	5.3.1.7.2.6 (4)	WAB TP IO-12
17	The introduction of a WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008, Section 5.2.12.6, DoD Secure Communications Devices (DSCD).	5.3.1.7.2.6 (5)	WAB TP IO-13
18	The WAB shall transport all call control signals transparently on an end-to-end basis	5.3.1.7.2.6 (6)	WAB TP IO-14
19	The addition of a WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period.	5.3.1.7.2.6 (7)	WAB TP IO-15
20	The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section	5.3.1.7.2.6 (8)	WAB TP IO-16
21	WLAS/WAB combination shall: - support Service Class tagging/QoS. - WAB may support special C2 calls, C2, C2(R), and non-C2 calls. All calls must meet other specified performance requirements for these users.	5.3.1.7.2.6	WLAS/WAB TP IO-17
ASLAN Requirements Applicable to Wireless Components			
22	All ASLAN C/D/A components must be non-blocking for a minimum of 50% rated output capacity.	5.3.1.3 (1)	WLAS/WAB TP IO-18
23	All ASLAN C/D/A components shall transport prioritized voice with no more than 2 ms latency.	5.3.1.3 (2)	WLAS/WAB Xref: IDs 6 and 19 (TPs IO-4 and IO-15)
24	All ASLAN C/D/A components shall transport prioritized voice with no more than 1 ms jitter.	5.3.1.3 (3)	WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. XRef: ID 20 (TP IO-16)
25	All ASLAN C/D/A components shall transport prioritized voice with no more than 0.02 % (C/D) and 0.01% (A) packet loss.	5.3.1.3 (4)	WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. TP IO-19
26	All ASLAN C/D/A components shall transport prioritized voice with no more than a BER of 1 bit error in 10^6 bits.	5.3.1.3 (5)	WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions TP IO-20
27	This test will demonstrate whether the device under test can receive alarms, policy violations, and performance issues.	5.3.1.6.4 & 5.3.2.17.3.1.5	WLAS/WAB TP IO-21
VoIP Device under Test Requirements Applicable to Wireless Components			
28	Supports VoIP device under test Codec for WEIs (G.711 with 20 ms).	5.2.12.8.2.2	WEI TP IO-22
29	Supports VoIP MLPP.	5.2.12.8.2.3	WEI TP IO-23

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	Remarks
VoIP Device under Test Requirements Applicable to Wireless Components (continued)			
30	VoIP Device under test latency 60 ms (+ 10 ms for wireless).	5.2.12.8.2.7	All XRef: ID 6**.** Averaged over any 5-minute period. The latency is to be measured from IP handset to egress from the VoIP device under test via a DSN trunk. TP IO-24
IA Requirements Applicable to Wireless Components			
40	The device under test shall be capable of using a static IP address.	5.4.6.2 (8)	All Table E-7, Test Case 15 TP IO-25
IPv6 Requirements Applicable to Wireless Components			
363	The device under test shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.3.5.3 (1)	WLAS/WAB Conditional -WEI Table E-13, Test Case 1 TP IO-26